Edith Cowan University

Copyright Warning

A Study of the Impact of the Affect Heuristic on the Risk Perception of Security Experts

Zack. A. Gurdon
BSc (Security) Hon

A Thesis Submitted to the Faculty of Computing, Health and Science
Edith Cowan University, Joondalup

In Partial Fulfilment of the Requirements for the Master of Security Management

Principal Supervisor: David Brooks

Submission Date: 21/11/2006

ABSTRACT

The management of security risk is widely viewed as a rational undertaking where accuracy is reliant upon the objective assessment of security experts. There is a traditional belief that experts have a greater understanding of objective 'risk'. However, when faced with uncertainty, both experts and laypersons rely on subjective mental frameworks, or heuristics, for making sense of complex environments. Where positive and negative *affect* such as feelings of 'good' and 'bad' are introduced to judgements, an *affect* heuristic can be demonstrated.

Utilising the psychometric paradigm as its theoretical framework, the study measured aspects of an *affect* heuristic in expert perception of security risk to establish whether there was an impact on judgements made in the risk assessment process. The psychometric factors of *dread risk* and *familiarity to risk* were utilised as the objective measures of risk perception toward security risk scenarios constructed with negative and neutral *affective* words. The results were then evaluated in light of the variations in perceived levels of dread and familiarity recorded for a sample population of 20 security experts.

The study demonstrated that the introduction of *affect* to security risk information did lead to variations in security risk experts' perceived levels of dread risk and familiarity to risk. As a result, the assessment of security risk could be considered subjective despite the expertise of the assessor. The study also showed that expertise created greater familiarity to risk, and as a result muted the influence of *affect*. The sample population believed the security risk scenarios to be *high dread risk* and *moderate familiarity with risk*.

Copyright and Access Declaration

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person accept where due reference is made in the text; or

(iii) contain any defamatory material

Signed _____ _____

Dated 15/12/2006

ACKNOWLEDGMENTS

I would like to acknowledge and thank Dave Brooks for pointing my research in the right direction at the outset, and for the guidance he provided during the completion of this thesis.

My thanks to Cliff Smith, Andrew Blades and Paul Bonny for taking time to critically review my study methodology.

My thanks go to Andrew Lester and his 3rd year security science students for allowing me to invade their lecture and then volunteering to assist in my pilot study.

Sincere thanks go to those security professionals who took time out of their busy schedules to actively participate in this study not just once, but twice.

My deepest and most sincere thanks go to my wife and son, Varsa and Krishan, for having the patience and fortitude to keep me focused on what I needed to do.

DEFINITIONS

Security "...implies a stable, relatively predicable environment in which an individual or group may pursue its ends without disruption or harm and without fear of destruction or injury" (Fischer & Green, 1992, p.3).

Risk "The chance of something happening that will have an impact on objectives" (Standards Australia, 2004).

Risk Management "The culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects" (Standards Australia, 2004).

Expert "Someone who is widely recognized as a reliable source of knowledge, technique, or skill whose judgment is accorded authority and status by the public or their peers" (Wikipedia Online Encyclopaedia, 2005).

Affect "A subjectively experienced feeling or emotion and the observable behaviour that represents it" (Fielder & Bless, 2001).

Heuristics "...mental rules of thumb for reasoning or educated guesses, which reduce or limit the search for solutions in domains that are ambiguous, complex and difficult to understand" (Shanteau, 1989).

Psychometric Paradigm	"An individual psychology-based research paradigm that aims to elicit judgments about risks from individuals who are confronted by risk stimuli" (Jackson, Allum & Gaskell, 2004).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Society's perception of 'risk' has undergone a significant transformation over the last century. 'Risks' are now widely perceived in many aspects of the physical and man-made environment. This reality is in stark contrast to the pre-industrialised era, where humanity's perception of risk did not extend beyond the next divinely imposed natural disaster or act of nationalistic conquest.

The 20th century proliferation in expert 'risk' research and public concern can be linked to the intellectual development of society, industrialisation and shift from the pre-modern to post-modern era (Lupton, 1997, p. 10). Society now has a plethora of regulatory bodies and institutions, all of which have been established to effectively manage risks resulting from the development of modern industry and technology. A greater need to manage societal risks has the consequent effect of making governance and technological control increasingly challenging.

Beck (1992) emphasises that this 'high modernity' is characterized by every citizen being exposed, to some degree, to technological dangers such as radioactivity, airborne and waterborne pollution, and hazards from mass transportation such as airline, automobile or train crashes. Consequently, despite enormous financial and intellectual effort being expended by governments and industry to make life safer and healthier, society has grown more, rather than less concerned about 'risk' (Slovic, 2001).

Background

Even as increasing industrial and technological complexity has required experts to develop objective measures for the assessment of 'risk', it has also bought about investigation into the influence of human psychology, society and culture on how human beings understand and perceive 'risk'. It can be argued that 'risks' are not objectively present in the environment, but are subjective creations mediated through cognitive, social and cultural influences (Thompson, Ellis & Wildavsky, 1990; Slovic, Fischhoff, & Lichtenstein, 1980).

The relevance of social risk theories has been repeatedly highlighted by the fact that individual perceptions of risk often do not appear to correlate with measurable probabilities of risk put forward by experts (Botterill & Mazur, 2004). For many experts, risk generally means expected annual mortality rates and probability of an impact (Morgan, 1993). However, for the layperson risk represents a more complex issue that also involves individualist factors like uncertainty, voluntariness, control, familiarity and dread, and contextual influences such as society and culture (Thompson et al, 1990; Slovic et al, 1980).

One particularly influential theoretical framework, the psychometric paradigm, proposes that a number of subjective factors directly affect how risk judgements by experts and laypersons take place (Slovic et al, 1980). Namely, the degree of dreadfulness in relation to an event, how familiar is the risk and finally the number of people exposed. The overall emphasis of the psychometric approach is that individual judgement of these factors takes place under the influence of psychological, social, cultural and institutional elements.

In the context of the psychometric paradigm, it can be argued that *both* experts and laypersons "objective" perception of risk are influenced by speculative and subjective mental frameworks referred to as heuristics. These 'mental shortcuts' are required for making sense of complex environments and undertaking judgements in uncertain situations (Botterill & Mazur, 2004; Kahneman, 2002). This study shows that where *affective* elements such as feelings of 'good' and 'bad' are introduced to 'objective' judgements involving risk, the presence of an *affect* heuristic can be demonstrated.

While the subjectivity in individual risk knowledge has been widely publicised and generally accepted in academic risk research, the prevailing practice by government and industry in Australia is that risk assessments can provide objective measures through rational and analytical means. This belief is demonstrated by the wide acceptance of formal risk management standards such as Australia/New Zealand Standard 4360: 2004 Risk Management (Standards Australia, 2004) by security, emergency and law enforcement agencies as their overarching risk management framework for operational, tactical and strategic activities.

However, it can be argued that the presence of an *affect* heuristic will actually result in the 'subjective' practice of "objective" risk management standards and principles. This subjectivity will be especially true in highly politicised cultures that manage emotive security issues such as terrorism, and where the popularity of "one size fits all" risk management models result in non-experts being given the responsibility of objectively assessing and managing risk (Australian Homeland Security Research Centre, 2005).

Study Significance

The management of security risk is widely viewed by government and industry as a rational undertaking where accuracy is reliant upon the objective assessment of security experts. Although there is a traditional belief that experts have a greater understanding of 'objective' risk, extensive social research over the last two decades has shown that experts themselves suffer from their own perceptions, bias and subjectivities (Sjoberg, 1999; Solvic, 2001). As such, 'objective' risk management can be viewed as largely subjective and assumption driven. This study demonstrated how *affect* as a heuristic impacts on security experts 'objective' risk perception.

By developing knowledge of how an *affect* heuristic and security risk perception interact, this study may also be able to provide security experts with an alternative theoretical foundation to enhance current 'objective' risk assessment practices. This outcome is significant in that the benefit would not only be valuable to security risk management practitioners in government and industry, but would also strengthen the relatively limited body of theoretical knowledge currently available to the security discipline.

Purpose of the Study

The purpose of this study was to measure aspects of the *affect* heuristic in expert perception of security risk to establish whether there is a meaningful impact on judgements made in the risk assessment process. The underlying risk characteristics of the primary psychometric factors of dread and familiarity were utilised as the objective measures of security expert perception and attitude toward risk. The impact of negative and neutral *affective* information about common security risks were then

evaluated in light of the variations generated in perceived levels of dread and familiarity.

By testing the target population of security experts, this research aimed to demonstrate that:

- An *affect* heuristic does influence security expert risk perception;
- The process of assessing security risk when *affect* is present is largely subjective despite the expertise of the assessor; and
- Intuitive rather than rational judgements are more likely when *affect* is present in security risk information.

Research Question

To determine whether an *affect* heuristic influences expert perception of security risk the following research question was addressed:

Does the introduction of *affect* to the communication of security risk information lead to variations in security risk experts' perceived levels of dread and familiarity?

To ensure the research question was appropriately examined, the following objectives were set forward for completion:

1. Construct semantic differential profiles (tabular representation) from the responses to neutral and negative security risk scenarios.
2. Independently discuss the semantic differential results from neutral and negative security risk scenarios.
3. Compare and contrast the semantic differential results from neutral and negative security risk scenarios.

4. Present semantic differential data in a spatial factor representation of dread and familiarity, and discuss.

Theoretical Background

The psychometric paradigm was selected as the theoretical foundation for this study. The large number of empirical studies producing common results from the paradigmatic approach attests to its viability as a theoretical framework for risk perception research (Jackson, Allum & Gaskell, 2004). As this study aimed to measure security expert risk perception, the psychometric paradigm and it use of psychophysical scaling, appeared to be well suited to this purpose.

Of particular relevance to this study were the paradigmatic concepts of dread and familiarity. These concepts not only provide a quantifiable structure to risk perception (Jackson et al, 2004), their inherently descriptive and emotive tone also mean *affect* can be measured and communicated in a manner that is conceptually aligned to 'emotion' and 'feelings'. Additionally, the use of dread and familiarity also captures the underlying emotive consequence of many security risks.

The important role of heuristics in risk perception also underpinned a significant theoretical component of this study. Krimsky (1992, p. 17) highlights this importance, when he argues that the risk characteristics identified in the psychometric paradigm can be considered judgemental heuristics in their function. Measurement of a concept that is already recognised as being integral to the psychometric paradigm, albeit a variation utilising *affect*, lent additional robustness to the significance and purpose of this research.

Overview of the Study

The study showed that the introduction of *affect* to the communication of security risk information did lead to variations in security risk experts' perceived levels of dread and familiarity. The psychometric factor space representation supported this outcome, with a meaningful variation between the neutral and negative security risk scenarios being evident. The sample population believed the scenarios to be *high dread risk* and *familiarity with risk.*

The central theme emerging from the interpretation of the final study was that expertise as well as an *affect* heuristic influenced the risk perception of security experts. The study showed that the 'familiarity' the sample population experienced toward the scenarios as a result of their expertise, muted the influence of *affect* on the familiarity factor.

Finally, the study outcomes demonstrated that meaningful results could be successfully applied in 'factor space' using the psychometric paradigm. The outcome was consistent with the viability of the paradigmatic approach and the large number of common results produced by empirical studies in risk perception. The study also showed that semantic differential scales and *affective* words could be applied as a valid and reliable instrument to measure sample population risk perception.

Study Limitations

This study's research instrument departed from the more conventional methodologies commonly applied in risk perception research. The validity and reliability of semantic differential scales that measure variations in dread and familiarity toward

security risk scenarios containing *affective* words cannot be supported by previous research methodologies. Although tests of reliably (Chronbach's alpha and paired-sample t-tests) were considered moderately acceptable, similar study outcomes would need to be replicated with the research instrument to demonstrate the on-going viability of the methodology.

Psychometric research is criticised for treating risk as purely objective, and not accounting for cultural or social bias hidden in the quantitative analysis (Shaw & Shaw, 2001; Lupton, 1997). The application of the psychometric paradigm for this study means the influence exerted by cultural and social agendas were not examined. Such an examination would have introduced contextual elements that could not be reliably interpreted within the theoretical framework or accurately represented in 'factor space'.

Empirical research into *affective* rationality is in its very early stages (Slovic, Finucane, Peters & MacGregor, 2004), and as a consequence, the ability to generalise study outcomes in relation to an *affect* heuristic is limited. To counteract this limitation, the study applied recognised psychological research principles to demonstrate the presence of an *affect* heuristic.

CHAPTER 2

LITERATURE REVIEW

The purpose of this literature review is to examine areas of knowledge, and take into consideration the impact this research may have upon the development of this study. Areas of research supporting this study are discussed under the following headings: Risk Perception; Heuristics and Rationality; Expertise and finally Research Methodology.

Risk Perception

Risk perception is subject to extensive debate in both academia research and industry practices. Despite a number of single theoretical perspectives of risk perception being put forward, none have been able to provide comprehensive and unified explanation or understanding of the concept. Lupton (1997) and Krimsky (1992, p. 15) suggest these risk perspectives exist on a continuum between constructionism and realism, and are theoretically expressed in individualist and contextualist approaches.

The most commonly accepted perspective remains the realist explanation for risk perception (Lupton, 1997). The realist perspective is reflected in the scientific and technical empiricism that objective risks exist as measurable properties in the environment. This philosophy is most frequently adopted by industry, and is reflected in the concept of risk as an expression of likelihood and consequence. Conversely, constructionism asserts that reality is only a subjective creation in which

risk does not exist independently of the individual, culture or society (Krimsky, 1992, p. 15).

The constructionist perspective of risk perception has much of its origins in Starr's (1969) seminal paper on social benefit versus technological risk. In this paper Starr attempted to reconcile the risk-benefit relationship through a "revealed social preference" approach, which assumes that the equilibrium between a risk and the benefit to society will reveal the overall acceptance of that risk (Fischhoff, Slovic & Lichtenstein, 1978). This outcome is established through the analysis of historical economic risk and benefit data, namely fatalities and individual spending, to identify patterns of acceptance.

Although subsequent analysis of the methodology has identified number of serious empirical deficiencies and problematic conclusions (Fischhoff et al, 1978), Starr's paper can be credited for introducing the concept of individualist perception to technical risk research. One study outcome of particular importance was that "...the acceptability of risk appears to be crudely proportional to...the real or imagined benefits" (Starr, 1969, p. 1234). The implications of this statement proved to be a catalyst for psychometric studies into the issue risk-benefit tradeoffs and public response to natural and man-made hazards.

The Psychometric Approach

Psychometric study is concerned with the measurement and objective evaluation of knowledge, abilities, attitudes, and personality traits in indivuduals (Lemon, 1973). In risk perception research, psychometric studies have identified that "perceived risk

is the outcome measurement of the interaction of an individual and the external environment mediated through cognitive structure" (Krimsky, 1992, p. 18). This perspective emphasises the rationality of human behaviour and the linear nature of cognitive processes in risk perception. Namely, there is knowledge of risk, leading to the development of individual attitude to risk and finally the adoption of a perspective on how the risk is understood (Lupton, 1997).

The dominant theoretical framework in this field is considered to be the psychometric paradigm, which uses psychophysical scaling and multivariate analysis to produce quantitative measures of risk attitudes and perceptions (Fischhoff et al, 1978). Measures of these attributes are considered to be directly 'expressed' preferences in attitude, as apposed revealed preferences through historic data proposed by Starr (1969). Fischhoff, et al. (1978) suggests the benefits of the psychometric approach to be identification of current individual preferences, sensitivity to changing values, and the consideration of subtle attitudes not available to probabilistic analysis.

To achieve a psychometric measurement of perceived levels of risk, benefit and acceptability, between nine to eighteen risk characteristics have been applied as 'attitude' structures against which individuals could quantitatively evaluate their perception. These risk characteristics were originally used by Slovic, et al. (1980) on the basis they represented concerns considered important by risk assessment researchers at the time. Through factor analysis, several strong colorations between these characteristics have established the presence of two dominating dimensions, dread and familiarity. These relationships are identified in *table 2.1*.

Table 2.1

18 Risk Characteristics and Factor Dimension Relationship

Dread		**Familiarity**	
Low Dread	High Dread	Familiar	Unfamiliar
Controllable	Uncontrollable	Observable	Unobservable
Not Globally Catastrophic	Globally Catastrophic	Known to those Exposed	Unknown to those Exposed
Consequence not Fatal	Consequence Fatal	Old Risk	New Risk
Equitable	Not Equitable	Effect Immediate	Effect Delayed
Individual	Catastrophic	Risks Known to Science	Risks Unknown to Science
Low Risk to Future Generations	High Risk to Future Generations	Little People Exposed	Many People Exposed
Easily Reduced	Not Easily Reduced		
Risk Decreasing	Risk Increasing		
Voluntary	Involuntary		
Doesn't Affect Me	Affects Me		

(Slovic et al, 1980 & Slovic, Fischhoff & Lichtenstien, 1986)

For the purpose of this study, the nine-risk characteristic approach is considered most applicable. The application of the expanded eighteen characteristic approach would be problematic, with characteristics such as 'high risk to future generations' and 'risk/benefit equity' having little obvious applicability to the immediate and generally pure risk nature of the security environment. The nine risk characteristics are identified in *table 2.2.*

Table 2.2

9 Risk Characteristics and Factor Dimension Relationship

Dread		**Familiarity**	
Low Dread	High Dread	Familiar	Unfamiliar
Controllable	Uncontrollable	Known to those Exposed	Unknown to those Exposed
Equitable	Not Equitable	Old Risk	New Risk
Individual	Catastrophic	Effect Immediate	Effect Delayed
Voluntary	Involuntary		

The qualitative measurements derived from the two-factor analysis of both the nine and eighteen risk characteristic models have yielded a number of foundation

understandings in risk perception (Krimsky, 1992, p. 18; Botterill & Mazur, 2004). Firstly, what constitutes an acceptable level of risk is higher for natural risks than for technology-based risks. Secondly, risk taking activities undertaken voluntarily and perceived to be "controllable" and "well known", such as driving or smoking, are perceived as less risky and more acceptable. Thirdly, risks thought to have catastrophic potential, have an uneven distribution of affect, and are unfamiliar to the public and experts, are generally rated as 'riskier', more probable and more serious.

When plotting dread and familiarity in factor space there is a clear indication that different types of risks are individually judged according to complex combinations of the above understandings (Botterill & Mazur, 2004). For example, nuclear power being located in the region of high dread and low familiarity (high risk) does not reflect the estimated probability of a nuclear hazard. Based on this quantitative assessment, it would be more reasonable to place this risk in close proximity to electrical power. The two-factor space model is identified in *figure 2.1*.

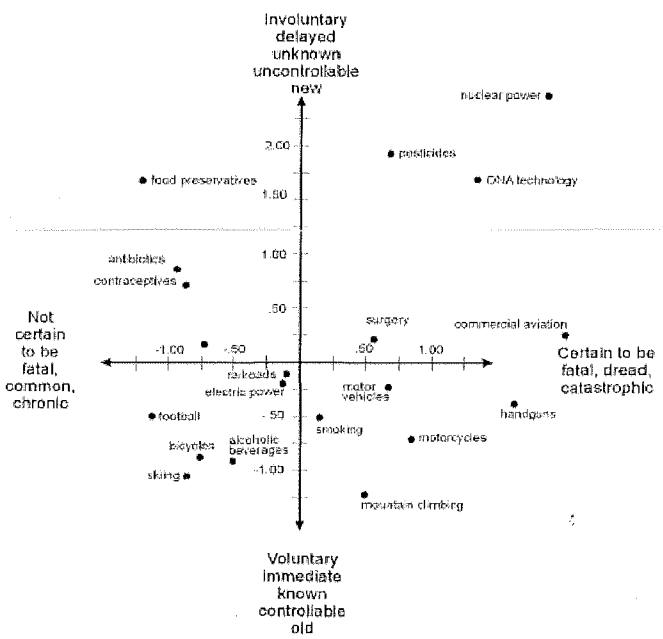

Figure 2.1 Two-Factor Space Model: Dread and Familiarity (Slovic et al, 1980)

Variations in how risk is understood have been prominently explained by the difference between expert and laypersons judgement of risk (Sjoberg, 1999). Early research by Slovic, et al. (1980) established that when experts judged risk there was a strong correlation with technical estimates of annual fatalities, while laypersons tended to be sensitive to the influences of dread and familiarity characteristics, leading to a considerable variation in levels of perceived risk. Although this perspective suggests experts have a simplistic and linear "understanding" of risk, Sjoberg (1999) argues that structure of expert perception varies little from the layperson. As a result, experts can be expected to be equally sensitive to external influences, such as the political agenda of the organisation or agency they represent.

Such external influence links to a key criticism of the psychometric paradigm, namely that the individualist approach does not consider risks in the social context in which they are experienced (Weyman and Kelly, 1999; Lupton, 1997, p. 23; Rayner, 1992, p. 75). Lupton (1997) asserts that while it is convenient for psychometric testing and modelling to represent individuals as "atomised" rational actors, it has had the affect of eliminating the impact of social context in individual risk perception. Social context, and whether or not it has a role in risk perception, represents the fundamental difference between the individualist and contextualist perspective.

Cultural Theory

Cultural Theory represents the dominant contextualist explanation of risk perception. The approach originates from anthropological studies relating to the examination of ritual defilement in primitive religions and unity of shared experience these behaviours create in a society (Rayner, 1992, p. 91; Lupton, 1997; Douglas, 1967).

These studies implied that the acceptance or rejection of these practices is based on the association of an individual to a particular culture. The practice of these traditions can be viewed as a means of imposing order on what is an inherently untidy and unstructured way of life for many individuals.

The emphasis upon the primacy of the social group, rather than individual cognition, in the perception, definition and management of risk is a key hypothesis put forward in Cultural Theory. In this hypothesis exists the principle source of conflict between Cultural Theory and the Psychometric Paradigm, as to which represents the primary social theory of risk perception. For proponents of the Psychometric Paradigm, an individual will always perceive, define and manage risk according to qualitative judgements based on subjective properties (Slovic et al, 1986).

The two conflicting individualist and contextualist frameworks lend themselves to the old argument, "which came first the chicken or the egg?" In the case of the Psychometric Paradigm and Cultural Theory this argument could be stated as, "does an individual's psychology and behaviour define their socio-cultural alignment, or is an individuals cognitive processes determined by the socio-cultural background?" In the arena of social risk theories this argument raises the dilemma of the primacy of these dominate social theories (Krimsky, 1992, p. 7).

The key assumption that 'risks' are subjective constructs, rather than objectively present within the environment, is present in both Cultural Theory and the Psychometric Paradigm. The argument of which hypothesis has greater explanatory power is largely irrelevant, since the exclusiveness of either has relatively little impact upon the final outcome of how individuals and socio-cultural affiliation

perceive and treat risk. While human beings may subjectively construct risks as individuals, the nature of culture and society ensures that the individual will group with others who perceive risk in a like manner. As a consequence, cognitive risk perception can be expected to reflect the wider influence of that culture.

Social Amplification of Risk Framework (SARF)

The concept of social amplification of risk is based on the proposition that events pertaining to risks interact with psychological, social, institutional, political and cultural factors in ways that heighten or attenuate individual or social perception of risk (Kasperson, 1992; Renn, Burns, Kasperson, Kasperson & Slovic, 1992). Although the major psychometric and cultural risk studies have provided explanations in this area, the approaches and findings, as discussed previously, have been fundamentally conflicting at the most basic conceptual level (individual versus contextual).

SARF attempts to resolve this general disjuncture between realist, individualist and contextualist explanations of risk, by integrating research explanations and findings from these approaches (Petts, Horlick-Jones & Murdock, 2001). One of the principal risk research impasses the framework attempts to address is why some risks viewed as statistically low by experts, become a focus of wider social-political concern and activity, while other more potentially serious risks receive comparatively little social-political attention. Breakwell & Barnett (2001) emphasise that social risk issues are only examined in the context of risk consequences.

Social amplification of risk occurs when an event's information signals spread like 'ripples' beyond the immediate zone of impact to influence stakeholders largely removed from its direct influence (Renn et al, 1992). Signals are received, interpreted and passed on by social "agents", such as individual experts, the public, organisations or social groups. Signal changes may be undertaken by agents to strengthen the importance of a message or to reinterpret or elaborate available information into a more acceptable form before passing on to other agents (Kasperson, 1992; Renn et al, 1992). These signal changes serve to amplify or attenuate the amount of information about an event or risk. The SARF is identified in *Figure 2.2*.

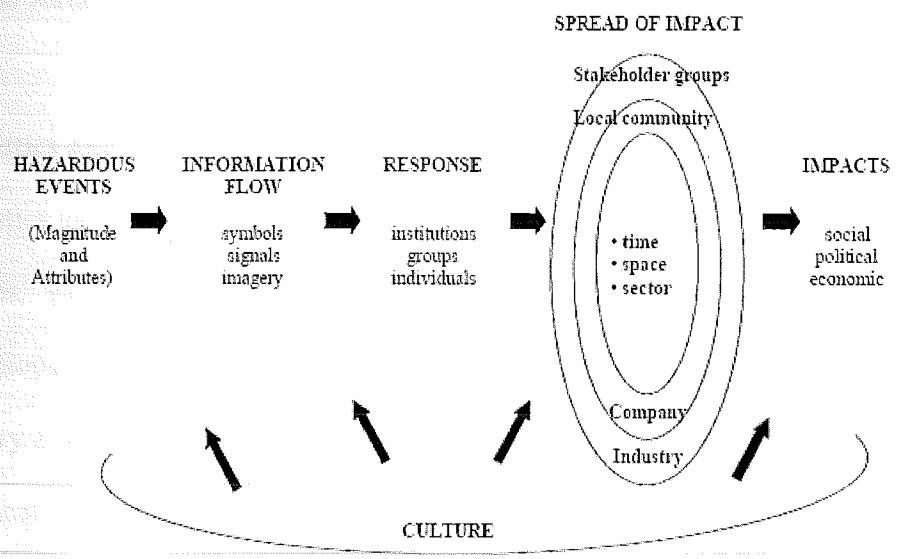

Figure 2.2 SARF
(Kasperson, 1992 cited in Petts et al, 2001)

SARF has particular relevance to the security environment, where there is an expectation that high profile risks such as terrorism will be managed to both institutionally and publicly acceptable levels. These expectations mean security experts are unlikely to "judge" risks in individualistic terms. It is more probable that

they will perceive "risk information according to the rules and expectations of their...organisation" (Renn et al, 1992, p. 8).

Such expectations imposed by an organisation are likely to be internalised and reinforced when an individual identifies with organisational goals, accepts institutional expectations and believes in the importance of how a risk should be judged (Renn et al, 1992). Petts, et al. (2001) and Renn, et al. (1992) contest that this social "colouration" significantly impacts individual perception by engendering patterns of understanding and the use of mental models for the future assessment of risks. This influence indicates the value of examining the relationship between attitude variations and the social context in which security risks are assessed.

Heuristics and Rationality

Heuristics are generally regarded as mental rules of thumb for reasoning or educated guesses, which reduce or limit the search for solutions in domains that are ambiguous, complex and difficult to understand (Shanteau, 1989; Solvic et al, 1980; Tversky & Kahneman, 1982, p. 3). Heuristics are contrasted by the use of probalistic, statistical or rationalistic reasoning, where systematic methods and processes are applied to solve problems, for the purpose of achieving optimal results.

In the area of risk and risk perception where judgements of probability and the prediction of values are a requirement, Tversky & Kahneman (1982, p. 3) argue that inherent complexity is reduced by a reliance on a limited number of heuristic principles referred to as Representativeness, Availability and Anchoring. Although Kahneman (2002) emphasises that these heuristics can be useful for guiding intuitive

decision-making, the subjectiveness of these judgements can result in severe and systematic errors. When undertaking risk assessments this process this can lead to serious incidents of bias and misrepresentation.

Heuristic Principles in Probalistic Judgement

Bar-Hillel (1982, p. 69) defines the representativeness heuristic as a "subjective judgement of the extent to which an event in question is similar in essential properties to its parent population". For example, an individual could be expected to judge *event B* as being as probable as *event A* whenever *B* appears representative of *A*. Although it would be reasonable to expect that the characteristics of *event B* would closely reflect *event A*, the presence of the heuristic means only a small element of *event A* needs only to be present for *event B* to be judged representative.

In the context of security risk, judgements based on representativeness suffer from insensitivity to reality. As an example, a crime trend involving vehicle ram raids targeting retail premises with external glass, could lead to a 'representativeness' judgement that all shops with windows onto the street are likely targets for this type of offence. However, individual circumstances, such as the close proximity of a 24-hour convenience store, would in fact significantly reduce the likelihood. In this instance, the representativeness heuristic will have led to a misrepresentation of the risk at this location.

The availability heuristic involves individuals "assessing the frequency of a class or the probability of an event by the ease with which instances or occurrences can be bought to mind" (Tversky & Kahneman, 1982, p. 11). Where 'availability'

judgements are made, there is little or no reference to the frequency or probability of previous related events. So where a high consequence low probability incident, such as a terrorist attack, takes place, the event's memorability will lead to an increase in the perceived 'risk' of future terrorist incidents. Such judgements mean the availability heuristic is a likely source of bias in risk perception (Slovic et al, 1980; Sunstein, 2005).

Further misrepresentation and inaccuracy can also be associated with the anchoring heuristic, which involves individuals' tendency to cause judgements to be anchored on initially presented values (Slovic et al, 1980). For example, in a study conducted by Kahneman (cited in Ariely, Loewenstein & Prelec, 2002), a wheel of fortune with numbers ranging from 0 to 100 was spun, and subjects asked whether the number of African nations in the United Nations was greater than or less than that number. The subjects were then requested to estimate the actual figure. Final estimates were significantly related to the number spun on the wheel (the 'anchor'), even though subjects could identify that the number had been generated randomly.

Dual Process Reasoning

Since the early research conducted by Tversky & Kahneman on heuristics, there has been an increased focus on the dual process relationship between rational decisions and intuitive judgements (Shafir & LeBoeuf, 2002). Unlike heuristics, which was originally viewed as a separate cognitive operation (Kahneman, 2002), dual process reasoning proposes that a heuristics-based holistic, *affective* and association driven (intuition) system coexists with an analytic, logical and reason oriented (reasoning)

system (Shafir & LeBoeuf, 2002; Kahneman, 2002; Sunstein, 2005; Slovic et al, 2004).

Intuition system operations are believed to be fast, automatic, effortless, associative and difficult to control or modify, while the reasoning system is characterised by slower, serial, effortful and deliberately controlled operations (Kahneman, 2002). Kahneman & Fredrick (cited in Sunstein, 2005) suggest that the two systems do not operate autonomously, but rather, the intuition system provides quick answers to problems of judgement, to which the reasoning system operates as a monitor, so the judgements can be confirmed or overridden. An adaptation of the two-system scheme is identified in *Figure 2.3*.

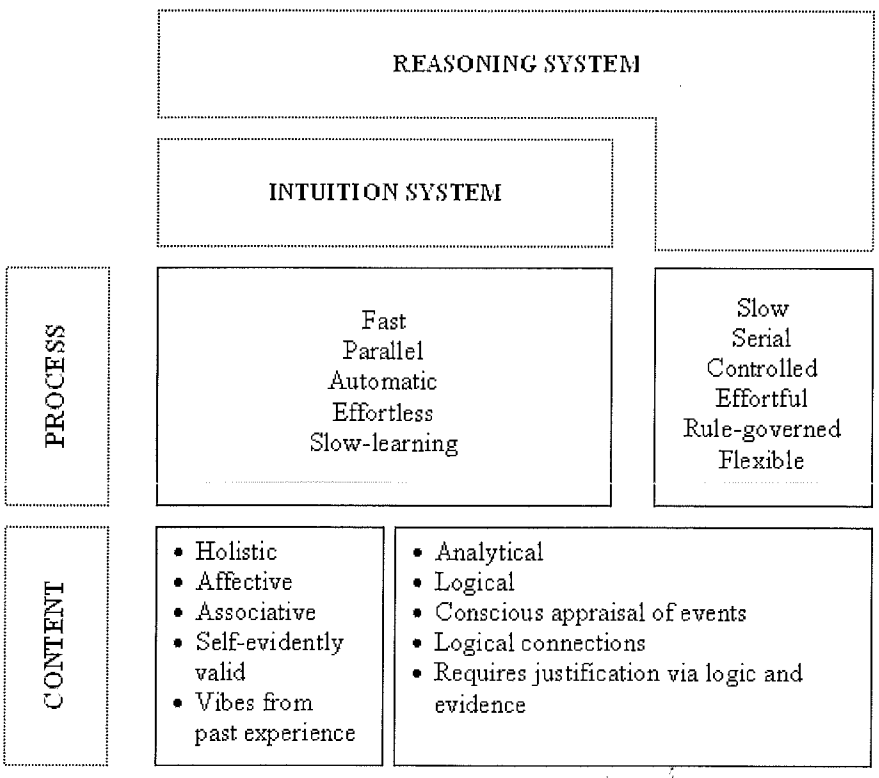

Figure 2.3 Two-System Scheme
(adapted from Slovic et al, 2004 & Kahneman, 2002)

One key proposition of the two-system approach is that the 'faulty' use of heuristics will not automatically lead to errors in judgement (Sunstein, 2005). The monitoring provided by the reasoning system will, under certain circumstances, allow individuals to overcome errors resulting from the use of heuristics. Sunstein (2005) also highlights that the capability 'check and balance' operation will vary, with individuals in possession of highly developed reasoning systems being more likely to recognise errors in heuristic-based judgements. In relation to this study, these assumptions mean that the often strong analytical background required by security experts may lead to a reduced impact from the *affect* heuristic.

Affect and Judgement

Despite the implied importance of the 'reasoning' capability, Slovic, et al. (2004) argues that *affect* or emotion also has a central role in the operation of the two system scheme. This perspective emphasises that *affect* is the central reference point or source for all judgements undertaken by the intuition system (Svenson & Slovic, 2002; Finucane, Alhakami, Slovic & Johnson, 2000). Functionally, this means an object or event requiring a judgement will result in a recollection of specific *affect* qualities of 'goodness' or 'badness' associated with previous experiences. These feelings, either unconsciously or consciously occurring, are then transferred onto the object or event, creating an emotive 'vibration' in the judgement.

An explanation for the intrinsic role of *affect* in judgement can be found in the premise that conscious rational action is built on and guided by the basic biological structures of intuition, emotion and feelings (Damasio cited in Finucane et al, 2000). This explanation is reflected in the logical structure of the two-system scheme, where *affect* is involved in all judgments referred through the intuition and reasoning

systems. Ultimately, as Slovic, et al. (2004) emphasis, it is unlikely that analytical thinking could be rationally employed without the influence from *affect* during the judgement and decision making process.

Apart from *affect* having a foundation role within dual process reasoning, recent research indicates that *affect* may also act as a specific type of heuristic (Finucane et al, 2000; Kahneman, 2002). An *affect* heuristic is believed to occur when automatic and rapid *affective* responses to events and objects substitute an individual's more systematic, considered judgements (Slovic et al, 2004). Direct substitution is able to occur, because representations of objects and events are 'tagged' with *affect*, resulting in automatic responses to consciously or unconsciously recalled elements. Kahneman and Fredrick (cited in Kahneman, 2002) argue that 'substitution' is the foundation of the heuristic process, in which readily recalled attributes, such as *affect* or availability, substitute rational processes in the assessment of a judgment.

Support for an *affect* heuristic can be drawn from the risk perception model proposed by Sandman (1987), in which he argues that the factors of uncertainty, voluntariness, control, familiarity and dread all represent elements of a collective concept termed 'outrage'. In this model an individual is likely to make judgements about risk based on the level of 'outrage' experienced, not on a rational assessment of objective evidence. This behaviour may indicate that experiences associated with the *affective* quality of 'badness' lead to direct behavioural expressions of 'outrage'.

Affect and Communication

Given this study aimed to measure and evaluate the impact of an *affect* heuristic, there is a requirement to understand how *affect* is manifested in observable behaviour. Without a quantifiable observation it is problematic as to whether a valid and reliable measure could in fact be developed for an *affect* heuristic. An explanation for the observable presence of *affect* in behaviour can be found in linguistic theory, and specifically the Sapir-Whorf hypothesis (Bamberg, 1993).

The Sapir-Whorf hypothesis argues that language provides much of the necessary structure for thought processes to occur. Without the definition and context of words, cognitive objects associated with perceiving the world, such as *affect*, could not be translated or communicated in structured and rational manner. Manifestation of *affect* can be observed behaviourally in use of 'goodness' and 'badness' as expressions of feeling and emotion.

Since it is probable that words have *affective* qualities which impact on cognitive processes and objects (Bradley & Lang 1999), it appeared appropriate to use *affective* words as the observable and measurable component of an *affect* heuristic. This type of approach is supported by Bestgen (1994), who indicates that normative *affective* words have been successfully used in numerous studies designed to measure and evaluate the role of *affect* on cognitive processing.

To ensure the *affective* words used in this study were valid and robust in terms of their normative valence (emotional orientation), an *affective* word list (ANEW) was obtained from the Center for the Study of Emotion and Attention at the University of Florida. This word list is freely distributed for non-profit research purposes, and

contains a set of normative ratings for over 2000 tested words in the English language (Bradley & Lang 1999). The suitability of the ANEW list has been demonstrated by its widespread application in psychological research on *affect* (Flint, 2004; Kensinger & Corkin, 2003; Maeda, Piguet, Connally, Krendl & Corkin, 2004).

Expertise

Wikipedia Online Encyclopaedia (2005) defines an expert as someone who is widely recognized as a reliable source of knowledge, technique, or skill whose judgment is accorded authority and status by the public or their peers. This explanation closely reflects the legal definition provided by the Australian Corporations Act 2001 (Cwlth) in which an "expert, in relation to a matter, means a person whose profession or reputation gives authority to a statement made by him or her in relation to that matter".

Experts can be expected to have prolonged or intense experience through practice and education in a particular field. In specific fields the definition is established by consensus, meaning an individual does not require a professional or academic qualification to be accepted as an expert (Wikipedia Encyclopaedia, 2005). Eysenck and Keane (2004) support this definition by emphasising that expertise is developed through extensive practice and an accumulation of knowledge, rather than the presence of some basic individual capacity.

For the purpose of this study, security experts are considered as such if they undertake risk assessments as part of their normal organisational/consultancy duties as a security advisor, manager, analyst or industry consultant. The objective

requirement for 'expertise' will be achieved using a criterion based on the ASIS International (2005), Certified Protection Professional (CPP) accreditation:

- Nine years of experience in a self managed security role; or
- Five years of experience in a self managed security role and a Bachelor Degree (ASIS International, 2005).

Sjoberg (1999) suggests that experts, regardless of their field, do not practice or apply their knowledge without bias. Rather they fulfil Protector and Promoter roles in society that represent individualist or collectivist ideals. The "Protector" considers their role to be the provider of warnings about risks that people have not considered or do not consider seriously enough. Conversely, the "Promoter" is focused on reassuring people that risks are not as bad or are safer than they appear. These roles again indicate that social context is a significant factor in determining how risks are perceived and ultimately addressed.

Research Methodology

Leedy (1997, p. 9) states that research methodology has two primary functions. Firstly, "to control and dictate the acquisition of data", and secondly "to capture the data after acquisition and extract meaningfulness from them". To be effective, the chosen research methodology for this study must meet two key criteria:

1. Provision of accurate and meaningful measurement of security experts' attitude toward risk.
2. Allow for the identification and quantification of the *affect* heuristic in security experts' attitude toward risk.

Creswell (1994), Preece (1994) and Leedy (1997) indicate that research is aligned into quantitative or qualitative paradigms. Creswell (1994, p. 1) defines qualitative research "as an inquiry process of understanding a social or human problem...formed with words, reporting detailed views of informants in a natural setting". Conversely, quantitative study is defined as "an inquiry into a social or human problem, based on testing a theory composed of variables, measured with numbers, and analysed with statistical procedures in order to determine whether predictive generalisations of theory hold true" (Creswell, 1994, p. 1).

These two definitions are sufficiently comprehensive to allow an appropriate method of research for this study to be determined. A quantitative approach is deemed inappropriate, since it is based on "testing a theory...measured with numbers and analysed with statistical procedures". This study will utilise a qualitative approach, since there is an "inquiry process of understanding a...social problem...this is formed with words".

Attitude Measurement

Slovic (1992, p. 121) identifies perception and attitude as independent factors to be measured and evaluated in the psychometric paradigm. However, despite the stated independence, there is no demarcation between perception and attitude in this model. This usage is representative of the stance taken in social psychology, in which perception and attitude are regarded as separate cognitive functions, but at the same time highly interdependent elements in the formation of knowledge structure (Fiedler & Bless, 2001, p. 122). The affect of this interdependence on psychological testing is such that a measurement of attitude is generally viewed as an equal measurement of

perception. Given the availability of tools for measuring attitude, for the purpose of this study, attitude has been chosen as the measure of risk perception.

Lewin (1979) and Thorndike (1997) suggest that anything, including attitude, can be measured. However, unlike statistically orientated data, measurement and evaluation of attitude cannot be achieved in a conclusive manner. Researchers may only make inferences about attitude from an observable indicator, such as a response to a statement, or the observation of an individual's overt behaviour (Anderson, 1988, p. 423). Such indicators represent manifestations of attitude, which must then be measured against a defined dimension.

Two major weakness associated with attitude measuring instruments is the ease in which they can be constructed and the indirectness of measurement through the use of verbal statements to make inferences about 'real attitudes' (Thorndike, 1997; Anderson, 1988, p. 425; Burns, 1997). In response, Oppenheim (1986) and Kifer (cited in Anderson, 1988, p. 424) emphasis practicing the following principles of measurement during instrument construction:

1. Identify the specific characteristics of the target concept against which attitude will be measured.
2. Achieve homogeneity or the focus on one concept at a time; confusion over the contents of an item weakens the reliability and validity of the instrument.
3. Apply linearity and equal appearing intervals; a scale provides a scoring system for statistical purposes and measurable dimensions for attitude concepts.

The importance of linearity dictates that, in most circumstances, attitude measurement is undertaken through the application of a scale (Burns, 1997; Oppenheim, 1986). The three most commonly used scaling techniques are the Likert method, the Thurstone scale and the Semantic Differential (Hopkins, Stanley & Hopkins, 1990; Burns, 1997). The wide acceptance of the Likert and Thurstone scales mean it would be appropriate to apply either one of these instruments for this study (Anderson, 1988, p. 427; Thorndike, 1997; Lewin, 1979; Hopkins et al, 1990). However, the psychometric paradigm use of contrasting adjectives to describe the dread and familiarity risk characteristics lends substantial weight to the application of the Semantic Differential.

The Semantic Differential

The Semantic Differential measures an individual's reaction to stimulus words and concepts with ratings on bipolar scales defined with contrasting adjectives at each end (Heise, 1970; Burns, 1997; Lemon, 1973; Nachmias & Nachmias, 1992). Words are selected for each scale on the basis they capture the range of attitude intensity toward an object. For example, semantic differential scales measuring individual attitude toward the concept of 'myself' may utilise adjectives such as good-bad, rigid-flexible and independent-submissive (Burns, 1997).

Early semantic differential research, which evaluated large numbers of adjective combinations, established that ratings on bipolar adjective scales tend to be highly correlated toward three basic dimensions commonly referred to as Evaluation, Potency and Activity factors (EPA conceptual framework) (Heise, 1970; Burns, 1997; Lemon, 1973). The central concepts of the EPA framework can be represented

by the adjective scales of good-bad for Evaluation, weak-strong for Potency, and fast-slow for Activity.

The Evaluation factor is considered the most critical dimension, because it directly estimates an individual's attitude toward an object (Burns, 1997; Lemon, 1973). The Potency and Activity factors are generally considered supporting dimensions that increase the overall accuracy of the scale. Typically, a concept is rated on several scales associated with a single dimension, with the results averaged to provide a single factor score for each dimension (Heise, 1970). An example of a semantic differential scale measuring individual attitude toward their customer service experience is identified in *Figure 2.4.*

	Very Much	Somewhat	Neither	Somewhat	Very Much		
	1	2	3	4	5		
helpful	○	○	○	○	○	unhelpful	Evaluation Factor
friendly	○	○	○	○	○	unfriendly	Potency Factor
polite	○	○	○	○	○	rude	Potency Factor

Figure 2.4 Semantic Differential Scale (University of Maryland, 2005)

Conclusion

The dominant theoretical framework in risk perception research is considered to be the psychometric paradigm. For the psychometric paradigm to achieve a measurement of perceived levels of risk, between nine and eighteen risk characteristics have been used as 'attitude' structures against which individuals quantitatively evaluate their perception. Through factor analysis, several strong colorations between these characteristics have established the presence of two overarching dimensions, dread and familiarity.

Early research using the psychometric paradigm established that when experts judged risk there was a strong correlation with probabilistic data, while laypersons were sensitive to the influence of dread and familiarity characteristics. More recent research argues that expert perception varies little from the layperson, since expertise is developed through extensive practice and an accumulation of knowledge, rather than the presence of some basic individual capacity. This means experts are also equally sensitive to external influences in complex judgements, such as those proposed by the social amplification of risk framework (SARF).

Where judgements of probability and the prediction of values are required, it is argued that inherent complexity is reduced by a reliance on heuristic principles and the dual process relationship between rational decisions and intuitive judgements. Dual process reasoning proposes that a heuristics-based holistic, *affective* and association driven (intuition) system coexists with an analytic, logical and reason oriented (reasoning) system. It is argued that the two systems do not operate autonomously, but rather the intuition system provides quick answers to problems of judgement, to which the reasoning system operates as a monitor.

While it is argued that *affect* or emotion has a central role in the operation of the two system scheme, recent research also indicates that *affect* may also act as a specific type of heuristic. An *affect* heuristic is believed to occur when automatic and rapid *affective* responses 'substitute' more systematic, considered judgements. Direct substitution is able to occur, because representations of objects and events are 'tagged' with *affect*, resulting in automatic responses to recalled elements. Substitution is the foundation of the heuristic process, in which readily recalled

attributes, such as *affect* or availability, substitute rational processes in the assessment of a judgment.

To evaluate the impact of an *affect* heuristic, there is a requirement to understand how *affect* is manifested in observable behaviour. Without a quantifiable observation it is problematic as to whether a valid and reliable tool could be developed for an identifying an *affect* heuristic. Since it is commonly accepted in psychological research that words have *affective* qualities which impact on cognitive processes and objects, it is appropriate for this study to use *affective* words as the observable component of an *affect* heuristic. The measurement of which will occur through the application of semantic differential scales.

CHAPTER 3

STUDY METHODOLOGY

Study design is guided by the research problem and the nature of the research questions being investigated (Moore, 2000). As the purpose of this study was to assess the impact of the *affect* heuristic on security expert risk perception, the methodology adopted was a qualitative approach that utilised research instruments to measure attitude.

Study Procedure

In selecting a qualitative approach, Isaac & Michael (1995) suggest that a functional study procedure should follow a descriptive format. The purpose of this type of procedure is to describe systematically, based on the research questions, the attitudes and characteristics of a given population in a factual and accurate manner. In order to reflect these attributes, the research process constituted the following stages identified in *figure 4.1.*

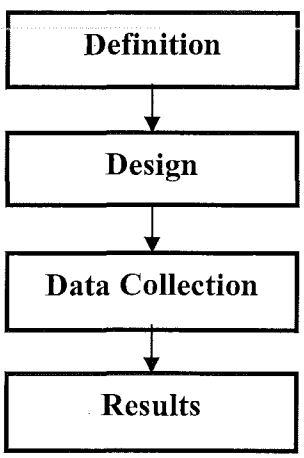

Figure 4.1. Research Procedure

Definition

The study was defined through the communication of a specific research question and a comprehensive review of existing research during the literature review. This process of definition and exploration enabled specific and achievable research objectives to be developed, which in turn, when addressed, allowed the research question to be appropriately and rigorously examined.

Design

The study design focused on the use of seven-point semantic differential scales (Best & Kahn, 1998; Lemon, 1973), which are similar to Likert scales in that respondents indicate an attitude between two extreme choices (Best & Kahn, 1998, p. 319). The semantic differential scales measured the sample population's attitude toward seven of nine risk characteristics identified by Slovic, et al. (1978) as comprising the factors of dread and familiarity.

Table 4.1

Measurable Risk Characteristics

Dread		**Familiarity**	
Low Dread	High Dread	Familiar	Unfamiliar
Controllable	Uncontrollable	Old Risk	New Risk
Equitable	Not Equitable	Effect Immediate	Effect Delayed
Voluntary	Involuntary		

(Fischhoff et al, 1978 & Slovic et al, 1986)

The semantic differential was selected as the principal research instrument, because it closely aligned to the extreme choices available to the risk characteristics listed above. For example, a standard semantic differential adjective of good-bad and the

risk characteristic of low dread-high dread both capture an extreme range of attitude intensity in one scale. The seven scale semantic differential is identified in *figure 4.2.*

Low Dread								High Dread
Controllable								Uncontrollable
Equitable to those Exposed								Not Equitable to those Exposed
Voluntary								Involuntary
Familiar								Unfamiliar
Old Risk								New Risk
Effect Immediate								Effect Delayed
	1	2	3	4	5	6	7	

Figure 4.2 Risk Characteristic Semantic Differential Scales

The seven semantic differential scales were designed to elicit attitude responses from the sample population to a series of security risk scenario. Each scenario focused on providing risk information for common and unique security issues, specifically robbery, assault, expatriate safety and industrial espionage. The purpose of selecting common and unique risks was to evaluate whether 'uniqueness' and 'profile' had an impact on attitude intensity (Appendix A – original security risk scenarios).

The security risk scenarios were constructed with negative and neutral *affective* words linking analytical information in the form of 'objective' observations of each risk issue. The *affective* words were applied for the purpose of creating a neutral and negative orientation toward the scenarios. For example, a statement that "the police record a moderate level of assault in the local area" has a neutral orientation. However, if assault is substituted for violent crime, the statement tends to become negative. The *affective* words used in the final test scenarios were taken from the *affect* word list (ANEW), obtained with approval from the Center for the Study of Emotion and Attention at the University of Florida.

To enable the impact of the *affect* heuristic to be evaluated, two measurable versions of each scenario were developed. One version was orientated with neutral *affective* words and the other negative *affective* words. The neutral scenario aimed to create an attitude statement that was minimally influenced by *affect*, while the negative scenario utilised *affect* so as to introduce elements of the *affect* heuristic. The negative scenario's measurements were then compared against the measurements of the neutral scenario to identify variations in levels of dread and familiarity. The presence of a variation would indicate an impact from the *affect* heuristic.

Both versions of each scenario were applied to the sample population. To address the issue of contamination due to scenario recollection, the test was applied in two stages separated by a six-week period. A combination of neutral and negative scenarios were provided in each stage. Although Nachmias & Nachmias (1992, p. 165) and Burns (1997) suggest that eight weeks is the minimum length of time between such re-tests, the limited timeframe available for this study meant a compromise period was required (Appendix B – Final security risk scenarios).

Data Collection

This stage of the research process consisted of the following steps:

Stage 1: Test Development – Study Feasibility

1. A pool of neutral and negative security risk scenarios to measure the impact the *affect* heuristic on the risk perception of security experts were developed.
2. Security risk scenarios submitted to appropriate security experts to evaluate face and content validity.
3. Security risk scenarios that lacked face and content validity were modified.

4. Finalised security risk scenarios were submitted to a 3rd year Security Science class at two different times, approximately 2 weeks apart.
5. Reliability tests of Chronbach's alpha and paired sample t-tests were applied to the security risk scenarios.
6. The security risk scenarios that failed to produce meaningful results and returned unacceptable reliability scores for the pilot study were removed from the final study.

Stage 2: Administer Test – Final Phase

7. The remaining security risk scenarios were ordered into a Final Test and packaged for distribution to the sample population.
8. Test One containing questionnaire part one was administered to the sample population.
9. Test Two containing questionnaire part two was administered to the sample population approximately 6 weeks after the first.
10. The results were compiled and analysed.

Results

The semantic differential results for the assault and expatriate safety scenarios were examined individually and then compared as dread and familiarity representations in 'factor space'. An analysis of the dread and familiarity factors established if the sample population reactions supported or rejected the research question. Specifically, data interpretation occurred in four parts:

1. Semantic differential profiles were constructed from the results of the neutral and negative security risk scenarios.

2. Semantic differential results from each security risk scenario were discussed independently.
3. The semantic differential results from the security risk scenarios were compared and contrasted.
4. The semantic differential results were presented in a spatial factor representation of dread and familiarity and discussed.

Sample Population

The sample population in this study were comprised of security experts from government and industry who undertake security risk assessments as part of their normal organisational/consultancy duties as a security advisor, manager, analyst or industry consultant. To ensure the requirement for 'expertise' was addressed, the sample population was selected using a criterion based on the ASIS International (2005), Certified Protection Professional (CPP) accreditation:

- Nine years of experience in a self managed security role; or
- Five years of experience in a self managed security role and a Bachelor Degree.

A homogeneous non-probability sample of at least 20 security experts was selected for this study. The high degree of specialisation required for experts in the field of security, limited variations in the representativeness of the sample population. The respondents for this study were identified through peer networks and professional associations in the security industry. To maintain the integrity of the expertise criteria, the following controls were implemented for respondent suitability:

- The eligibility criterion was outlined in the test pack, and the respondents advised that they should only complete the survey if they meet the criteria.

- Respondents were required to note their experience and qualifications against the criteria before their responses will be accepted.

Initial distribution of the test pack occurred through email to a list of security experts previously identified as meeting the expertise criteria. These individuals were known personally through professional relationships and ASIS International Australian Chapter participation. There was no geographical limitation on distribution, with respondents coming from both domestic and international locations.

Each respondent was asked to distribute the test pack to other security colleagues, who to their knowledge met the expertise criteria and for whom English was their first language (to maximise consistent interpretation). All respondents were requested to return Test One in electronic format by return email. A record of all eligible respondents was maintained so that Test Two could be directly distributed after six weeks for completion and return.

Validity

Due to the lengthy research procedure it was considered unfeasible to apply more time consuming tests, such as construct validity. In this circumstance content and face validity were considered most appropriate. Both tests of validity were achieved by submitting the risk scenarios and semantic differential scales for examination to four security experts (two from academia and two from industry) to ensure they fulfilled their functional requirements.

Minor wording changes were identified with the questionnaire backgrounds and several scenarios. After modifications had been made, the test items were considered to be valid. At the conclusion of this process the Pilot Test was then conducted.

Reliability

Reliability of the test items was established by the application of Chronbach's alpha and paired-sample t-tests to semantic differential scales grouped under their factors of dread and familiarity.

Chronbach's alpha is a test for a model internal consistency; it assesses the extent to which a set of test items can be treated as measuring a single latent variable. The paired-sample t-test is used to determine if there is a meaningful difference between the means of two sample populations. Both tests were run through SPSS statistical software.

Limitations

This study, like any research project, has a number of limitations that have been identified from the research methodology and the results of the pilot study. Where possible, action was taken to reduce the negative impact upon the final test. The following is a description of the limitations facing the study.

The proposed sample size of 20-30 subjects does limit the ability to generalise outcomes of the study. The specialised profession of security experts allowed only limited number of subjects to be selected for the sample population. The resultant small sample size means that the attitudes assessed may not necessarily be

representative of the wider security expert population. This issue can only be overcome by collecting a sufficiently large sample population.

There are several limitations associated with inferring meaning from observable displays of individual attitude. For a test instrument to effectively measure attitude, the researcher depends upon expressed opinion that is a true reflection of the subject's belief. However, there is a probability that the subject may conceal their attitude behind socially acceptable opinion (Thorndike, 1997). Lewin (1979) also highlights that test items may present subjects or issues of which they have no knowledge.

Psychometric research has been criticized for treating risk as purely objective, and not accounting for cultural or social bias hidden in the quantitative analysis (Shaw & Shaw, 2001; Lupton, 1997). Given security experts operate in environments where strong social agendas form from highly politicised and emotive issues such as terrorism, the application of the psychometric paradigm for this study means the influence exerted by social agendas may not be accounted for. Although this limitation is inherent to the individualist approach, and in the context of this study, largely unavoidable, it is offset to some degree by the proven viability of the paradigmatic approach as a theoretical framework (Jackson, Allum & Gaskell, 2004).

CHAPTER 4

PILOT STUDY

A pilot study was undertaken to evaluate the suitability and reliability of the proposed security risk scenarios for assault, industrial espionage, robbery and expatriate safety. Secondary benefits of the pilot study included feedback from the sample population on the readability and lucidity of the test item instructions and scale construction.

3rd year security science students from Edith Cowan University were selected as the sample population for the pilot study. This particular population was selected on the basis that:

- they would possess a similar *theoretical* knowledge structure of the security discipline, including security risk, to that of security 'experts'; and
- they would not draw from the limited field of security experts eligible to participate in the final study.

Data Collection

Test one, containing all neutral scenarios, was provided in person to a class of 3rd year security science students for voluntary completion. The ten participating students took between 15-25 minutes to complete the first test. The test was finalised with the students being requested to provide written feedback on the general 'useability' of the test item. Students were also requested to record their name and email address so the second test could be distributed electronically.

Approximately three weeks after the initial test the second test was distributed by email to the participating students. Of the original ten participants, six completed and returned the second test in electronic format. Several attempts were made to contact the remaining students, but no responses were forthcoming. Although the final pilot study sample size was small, the response rate of 60% is considered acceptable in social research (Babbie, 1995).

Data Collation

The results from the pilot study were analysed to determine the reliability of the semantic differential scales and the security risk scenarios. The data analysis phase involved the following steps:

1. The scores from each neutral and negative semantic differential scale were collated into four tables for the scenarios of assault, industrial espionage, robbery and expatriate safety (Raw Data Table – Appendix E).
2. The mean and standard deviation for each neutral and negative semantic differential scale were calculated from the responses to both the first and the second test.
3. The semantic differential scales for each scenario were grouped by the factor of dread (dread, control equity and voluntariness) and familiarity (familiarity, old/new and immediacy).
4. A consolidated mean for the dread and familiarity factors were calculated from the mean of the grouped semantic differential scales.
5. Internal consistency of the dread and familiarity factors for each scenario were tested using Chronbach's alpha (run through SPSS).

6. Paired sample t-tests were undertaken of the dread and familiarity factors to identify the statistical significance between the neutral and negative scenarios (run through SPSS).

Assault Scenario Data

The sample population's reaction to the neutral and negative assault scenario resulted in an increase in dread and unfamiliarity for six of the seven 7-point semantic differential scales (1=low dread/highly familiar and 7=high dread/very unfamiliar). Mean score increases were recorded for dread (5.17 [SD 0.75] to 5.83 [SD 0.98]), control (3.83 [SD 1.72] to 4.17 [SD 1.94]), equity (4.50 [SD 1.64] to 6.33 [SD 0.52]), familiarity (2.83 [SD 1.72] to 3.33 [SD 1.86]), old/new (2.33 [SD 1.37] to 3.17 [SD 1.47]) and immediacy (1.67 [SD 0.52] to 2.33 [SD 1.03]), while voluntariness (5.50 [SD 1.05] to 5.17 [SD 1.83]) recorded the only mean score decrease or inverse relationship. The 'semantic differential profile' for the neutral (green) and negative (red) assault scenario is identified in *figure 5.1*.

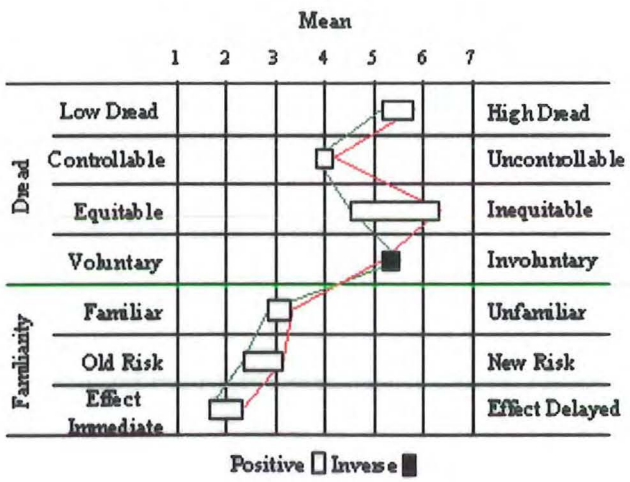

Figure 5.1 Semantic Differential Profile – Assault Scenario

A consolidated neutral and negative mean score for both factors was calculated using the grouped neutral and negative mean scores from each semantic differential scale.

The dread factor risk characteristics of dread, control, equity and voluntariness combined to produce factor mean score increase of 4.75 [SD 0.47] to 5.38 [SD 0.69]. The familiarity factor risk characteristics of familiarity, old/new and immediacy also combined to produce a factor mean score increase of 2.28 [SD 0.44] to 2.94 [SD 0.41]. The spatial factor representation of dread and familiarity for the neutral (green) and negative (red) assault scenario is identified in *figure 5.2.*

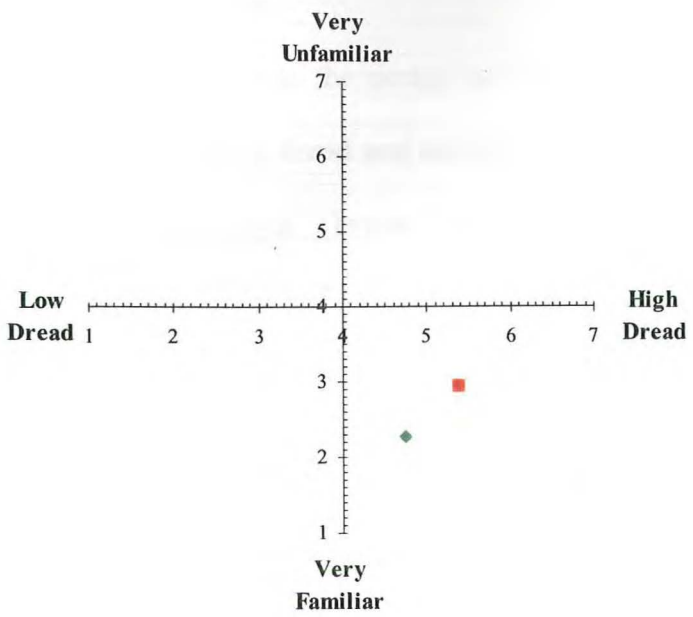

Figure 5.2 Factor Space – Assault Scenario

While the suitability of the assault scenario was supported by the meaningful variation in reaction intensity identified in 'factor space', an examination of reliability was also required before the scenario could be accepted for the final study. Chronbach's alpha and paired-sample t-tests were used to test the neutral and negative semantic differential scales when grouped by their dread and familiarity factors.

The assault scenario returned an *acceptable* (DeVellis, 1991) internal consistency coefficient of 0.76 and 0.80 for both the dread and familiarity factors respectively.

The paired-sample t-tests identified a statistically insignificant result for the dread factor [t (24) = .06, p>.05], but a statistically significant result for the familiarity factor [t (18) = .00, p<.05]. These results, combined with the meaningful variation in reaction intensity displayed in 'factor space', provide an adequate level of support for the assault scenario to remain in the final test.

Industrial Espionage Scenario Data

The sample population's reaction to the neutral and negative industrial espionage scenario resulted in an increase in dread and unfamiliarity for four of the seven 7-point semantic differential scales (1=low dread/highly familiar and 7=high dread/very unfamiliar). The neutral and negative mean scores for dread (6.17 [SD 0.75] and 6.17 [SD 1.17]) remained unchanged. Control (3.33 [SD 2.50] to 2.67 [SD 1.21]) and voluntariness (2.50 [SD 2.35] to 2.17 [SD 0.98]) both recorded mean score decreases or inverse relationships, while equity (2.83 [SD 2.48] to 4.33 [SD 2.07]), familiarity (2.67 [SD 1.37] to 3.00 [SD 1.41]), old/new (3.17 [SD 2.23] to 5.00 [SD 1.55]) and immediacy (4.67 [SD 1.97] to 5.00 [SD 2.19]) all recorded mean score increases. The semantic differential profile for industrial espionage is identified in *figure 5.3*.

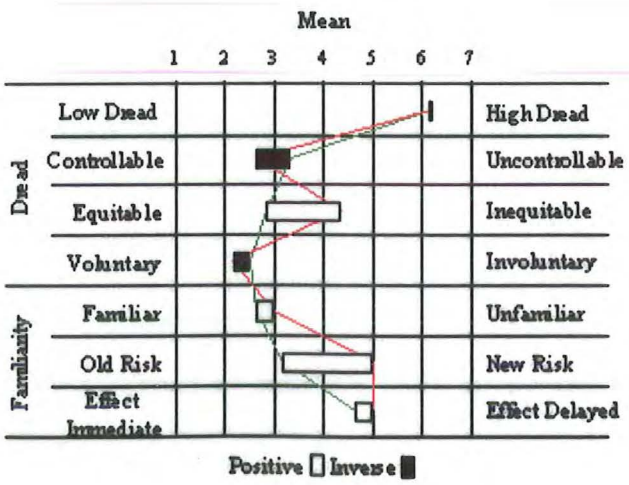

Figure 5.3 Semantic Differential Profile – Industrial Espionage

A consolidated neutral and negative mean score for the dread and familiarity factors was calculated using the neutral and negative mean scores of each semantic differential scale. The dread factor risk characteristics of dread, control, equity and voluntariness combined to produce factor mean score increase of 3.71 [SD 0.85] to 3.83 [SD 0.48]. The familiarity factor risk characteristics of familiarity, old/new and immediacy also combined to produce a factor mean score increase of 3.50 [SD 0.44] to 4.33 [SD 0.41]. The spatial factor representation of dread and familiarity for the neutral and negative industrial espionage scenario is identified in *figure 5.4*.

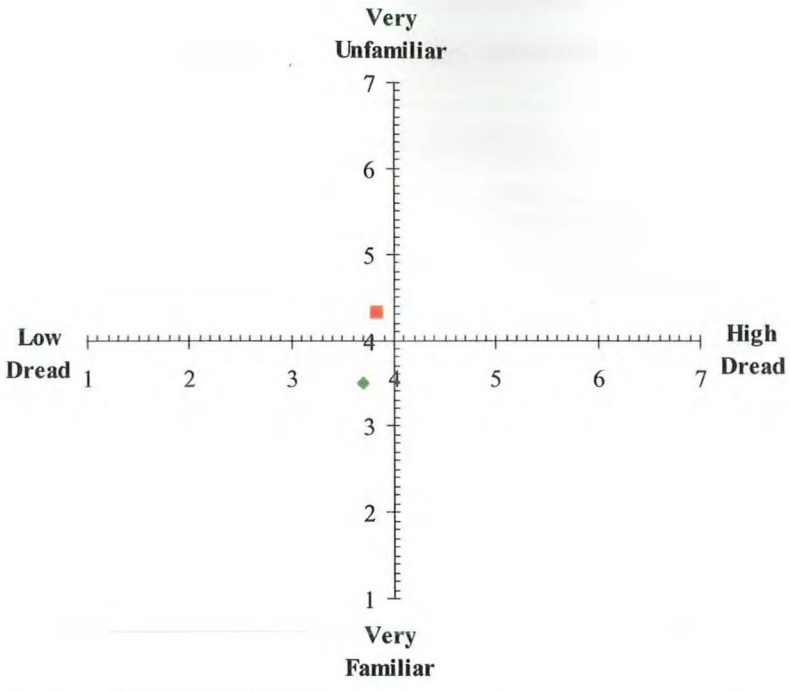

Figure 5.4 Factor Space – Industrial Espionage Scenario

The 'factor space' representation for the industrial espionage scenario displays a meaningful shift in reaction intensity for familiarity. However, there is little noticeable change in the level of reaction intensity for dread, with only a 0.12 increase occurring on a 7-point scale. This outcome suggested that the industrial espionage was unsuitable for the final test. To assess reliability, Chronbach's alpha

and paired-sample t-tests were used to test the neutral and negative semantic differential scales when grouped by their dread and familiarity factors.

The industrial espionage scenario returned *undesirable* (DeVellis, 1991) internal consistency coefficients of 0.47 and 0.40 for the dread and familiarity factors respectively, while the paired-sample t-tests identified a statistically insignificant result for the dread factor [t (24) = 1.00, p>.05] and familiarity factor [t (18) = .10, p>.05]. Given the lack of meaningful variation in reaction intensity for the dread factor, the results for alpha and t-tests failed to provide a sufficient level of reliability, and supported the withdrawal of the industrial espionage scenario from the final test.

Robbery Scenario Data

The sample population's reaction to the neutral and negative robbery scenario resulted in an increase in dread and unfamiliarity for only two of the seven 7-point semantic differential scales (1=low dread/highly familiar and 7=high dread/very unfamiliar). The neutral and negative mean scores for immediacy (2.00 [SD 1.26] and 2.00 [SD 1.10]) remained unchanged. Dread (6.33 [SD 0.52] to 6.00 [SD 0.89]), control (4.00 [SD 1.79] to 3.83 [SD 1.47]), voluntariness (4.50 [SD 1.52] to 3.83 [SD 1.83]) and familiarity (2.83 [SD 0.98] to 2.33 [SD 1.82]) all recorded mean score decreases, while only equity (4.83 [SD 2.48] to 5.83 [SD 1.17]) and old/new (2.00 [SD 0.89] to 2.17 [SD 1.47]) recorded a mean score increase. The semantic differential profile for robbery is identified in *figure 5.5*.

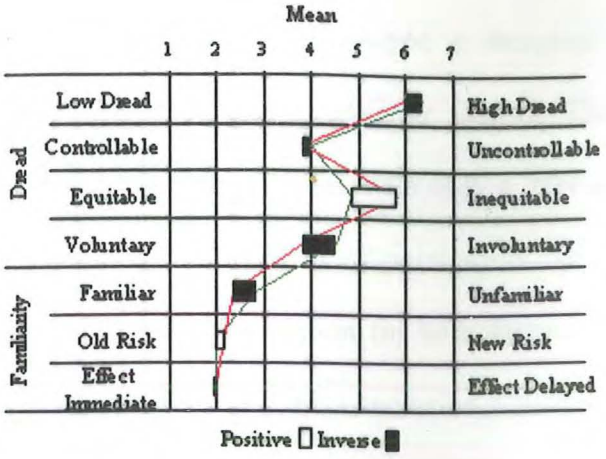

Figure 5.5 Semantic Differential Profile - Robbery Scenario

A consolidated neutral and negative mean score for the dread and familiarity factors was calculated using the neutral and negative mean scores of each semantic differential scale. The dread factor risk characteristics of dread, control, equity and voluntariness combined to produce a slight mean score decrease of 4.92 [SD 0.82] to 4.88 [SD 0.40]. The familiarity factor risk characteristics of familiarity, old/new and immediacy also combined to produce a slight mean score decrease of 2.28 [SD 0.19] to 2.17 [SD 0.33]. The spatial factor representation of dread and familiarity for the neutral (green) and negative (red) robbery scenario is identified in *figure 5.6*.

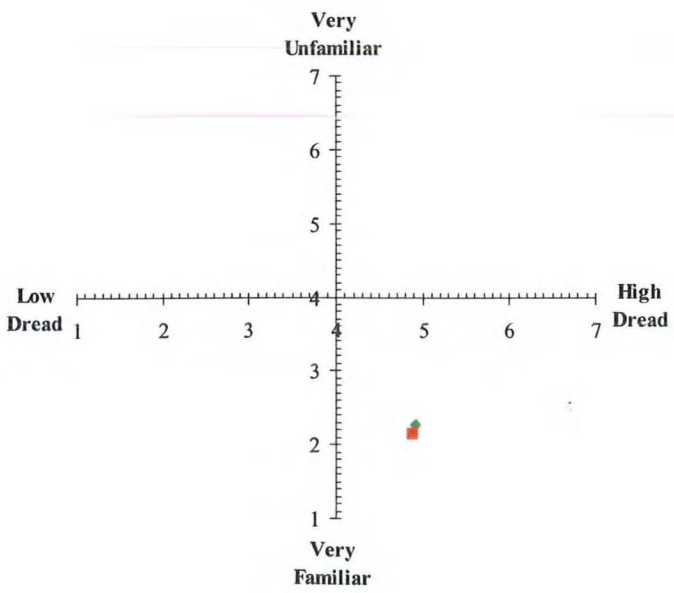

Figure 5.6 Factor Space – Robbery Scenario

The robbery scenario 'factor space' displayed a marginal negative or inverse relationship for both the dread and familiarity factors. The change in reaction intensity for both factors was insignificant, with only a 0.04 decrease for dread and 0.09 decrease for familiarity occurring on a 7-point scale. The failure of this scenario to produce a meaningful positive variation for both factors suggested it should be removed from the final test. To verify this conclusion, Chronbach's alpha and paired-sample t-tests were used to test the reliability of the neutral and negative semantic differential scales when grouped by their dread and familiarity factors.

The test of alpha returned an *acceptable* (DeVellis, 1991) internal consistency coefficient of 0.84 and 0.75 for both the dread and familiarity factors respectively. However, the paired-sample t-tests identified statistically insignificant results for both the dread factor [t (24) = .91, p>.05] and familiarity factor [t (18) = .61, p>.05]. While these outcomes indicate the neutral and negative scenario provided a high level of internal consistency (alpha), the results for statistical significance (p-value) reduce the scenario's reliability. These results, combined with the lack of meaningful variation in reaction intensity for the dread and familiarity factors, supported the withdrawal of the robbery scenario from the final test.

Expatriate Safety Scenario Data

The sample population's reaction to the neutral and negative expatriate safety scenario resulted in an increase in dread and unfamiliarity for six of the seven 7-point semantic differential scales (1=low dread/highly familiar and 7=high dread/very unfamiliar). Dread (5.50 [SD 1.87] to 6.33 [SD 0.52]), control (4.50 [SD 1.64] to 5.83 [SD 0.75]), equity (5.17 [SD 0.98] to 5.83 [SD 1.94]), voluntariness (4.17 [SD 1.83] to 5.00 [SD 2.00]),

familiarity (3.67 [SD 1.75] to 4.17 [SD 2.32]) and old/new (2.50 [SD 1.22] to 4.00 [SD 2.19]) all recorded mean score increases, while immediacy (2.67 [SD 1.86] to 1.83 [SD 1.17]) recorded the only mean score decrease or inverse relationship. The semantic differential profile for expatriate safety is identified in *figure 5.7*.

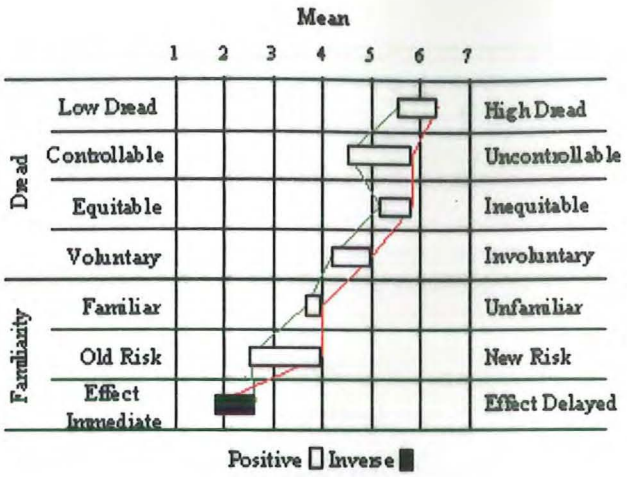

Figure 5.7 Semantic Differential Profile – Expatriate Safety Scenario

A consolidated neutral and negative mean score for the dread and familiarity factors was calculated using the neutral and negative mean scores of each semantic differential scale. The dread factor risk characteristics of dread, control, equity and voluntariness combined to produce a mean score increase of 4.83 [SD 0.41] to 5.75 [SD 0.78]. The familiarity factor risk characteristics of familiarity, old/new and immediacy also combined to produce a mean score increase of 2.94 [SD 0.34] to 3.34 [SD 0.63]. The spatial factor representation of dread and familiarity for the neutral (green) and negative (red) expatriate safety scenario is identified in *figure 5.8*.

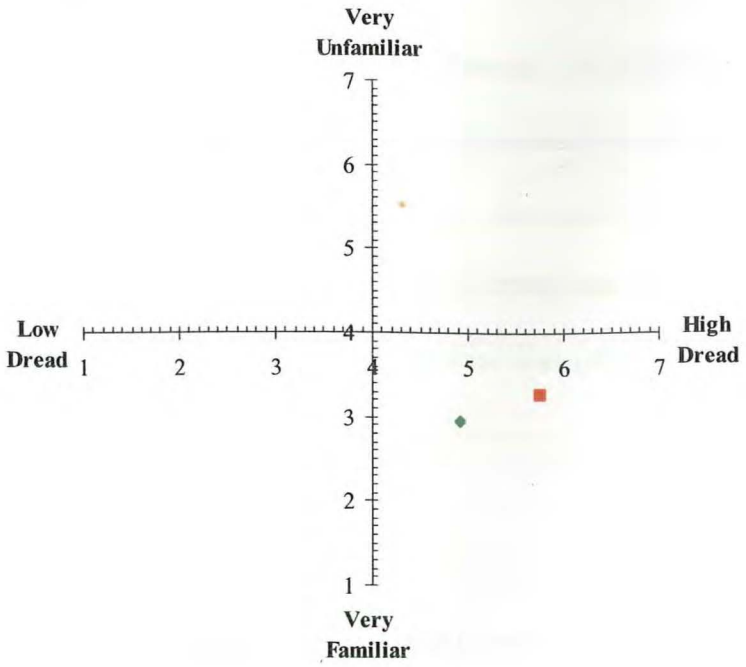

Figure 5.8 Factor Space – Expatriate Safety Scenario

The suitability of the expatriate safety scenario was supported by its 'factor space' representation, which displayed a meaningful variation in reaction intensity between the neutral and negative scenarios. To support this outcome, Chronbach's alpha and paired-sample t-tests were used to test the reliability of the neutral and negative semantic differential scales when grouped by their dread and familiarity factors.

The expatriate safety scenario returned an *acceptable* (DeVellis, 1991) internal consistency coefficient of 0.81 for dread, but an *undesirable* score of .41 for familiarity, while the paired-sample t-tests identified a statistically insignificant result for both dread [t (24) = .21, p>.05] and familiarity [t (18) = .75, p>.05]. While these results lacked a high level of reliability in both tests, the meaningful variation in reaction intensity displayed in 'factor space' provided sufficient support for the expatriate safety scenario to remain in the final test.

Data Analysis and Interpretation

The data interpretation discussion broadly addresses the research objectives set out for this project; being to discuss the semantic differential results from the neutral and negative security risk scenarios and to discuss the semantic differential data when presented in a spatial factor representation of dread and familiarity. The research objective to prepare semantic differential profiles was presented in the data analysis section.

Factor Space Discussion

The neutral and negative assault, robbery and expatriate safety scenarios all occupied the same spatial quadrant (lower right) of *high dread risk* and *familiarity with risk.* However, with industrial espionage, its neutral scenario occupied the *low dread risk* and *familiarity with risk* quadrant (lower left), while the negative scenario occupied the *low dread risk* and *unfamiliarity with risk* quadrant (upper left). These 'factor space' representations, identified in *figure 5.9,* suggested the presence of several underlying themes.

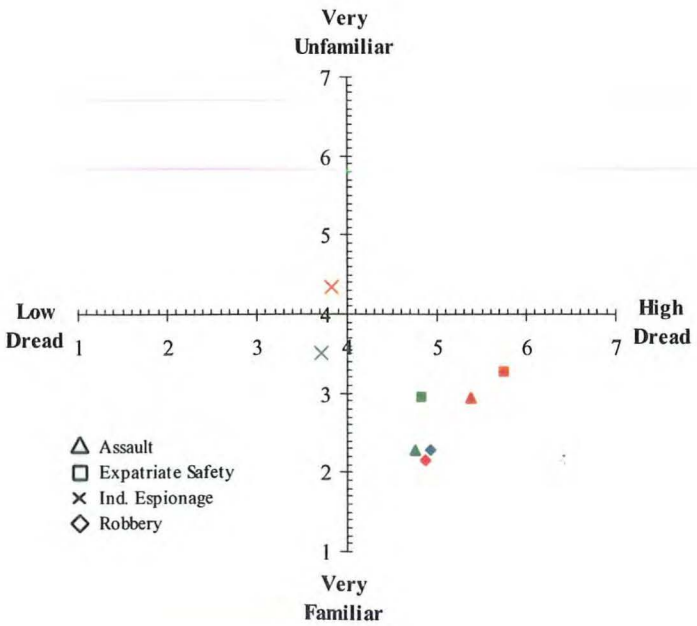

Figure 5.9 Factor Space – All Tested Scenarios

Where a 'person' was likely to be the 'victim' of a security risk, as in the case of assault, robbery and expatriate safety, higher levels of dread $^{(mean)}$ were experienced. However, where an entity was the 'victim', as in industrial espionage, the level of dread $^{(mean)}$ experienced was significantly lower. An explanation for this variation can be found in a fundamental security principle that proposes people to be more important than information and physical assets. Given the sample population were third year security science students, it could be expected that such a theoretical principle would influence their perception and assessment of security risk.

Industrial espionage was also unique in that it demonstrated a higher level of unfamiliarity in factor space, particularly for the negative scenario, when compared to assault, robbery and expatriate safety. This reaction was not unexpected, given the relative uniqueness of industrial espionage, its limited exposure in the public arena and the student sample population's lack of practical 'real life' experience in this area of security.

Assault Scenario – Discussion

Between the neutral and negative scenarios, the dread factor experienced a variation from *slightly* too *moderately* dreadful (4.75 to 5.38), while the familiarity factor experienced a variation from *moderately* too *slightly* familiar (2.28 to 2.94). In term of an overall response to the scenario, these outcomes indicate the sample population was largely familiar or comfortable in their knowledge of assault and its effects, but tended to be uncomfortable with the environment in terms of the likelihood and consequence of an assault.

Although the reactions to dread and familiarity were opposed to each other on the 7-point semantic differential scale, the variation between the neutral and negative scenarios for each factor was virtually identical, with 0.63 for dread and 0.66 for familiarity. While these variations were in themselves considered meaningful, such a small deviation between the two variances suggested the *affective* words had a similar impact on both the dread and familiarity factors.

Industrial Espionage Scenario – Discussion

The dread factor experienced a variation (mean total) between the negative and neutral scenarios that remained in the *neutral* dread range (3.71 to 3.83), while the familiarity factor experienced a variation that also remained in the *neutral* familiarity range (3.50 to 4.33). In terms of an overall response to the scenario, these outcomes indicated the sample population tended to be uncertain in their knowledge of industrial espionage and the impact of the scenario environment. This reaction was reflected to a large degree in dread, with a tendency toward uncertainty also being experienced. The orientation toward 'undecided' for both the familiarity and dread responses made this scenario unsuitable for the final test.

Robbery Scenario – Discussion

Between the neutral and negative scenarios, the dread factor experienced a variation that remained in the *slightly* high dread range (4.92 to 4.88), while the familiarity factor experienced a variation that remained in the *moderately* familiar (2.28 to 2.17) range. In terms of an overall response to the scenario, these outcomes indicated the sample population was for the most part certain in their knowledge of robbery. However, the fact that dread became slightly more *neutral* suggested risk

information in the scenario was conflicting or ambiguous, and as such precluded the sample population from forming a definitive attitude.

Expatriate Safety Scenario – Discussion

The dread factor experienced a variation between the neutral and negative scenarios from *slightly* tending toward *moderately* dreadful (4.83 to 5.38), while the familiarity factor experienced a variation that remained in the *slightly* familiar range (2.94 to 3.34). In terms of an overall response to the scenario, these outcomes indicated the sample population felt they had some knowledge of expatriate safety and its effects, but was largely uncomfortable with the environment in regard to the likelihood and consequence of an incident that may impact on expatriate safety.

Conclusion

Slovic et al (2004) argue that an *affect* heuristic occurs when automatic and rapid *affective* responses to events and objects substitute an individual's more systematic, considered judgements. Finucane et al (cited in Jackson, Allum & Gaskell, 2004) further contend that an *affect* heuristic is pervasive and extends to 'objective' numerical assessments of risk. These propositions appear to find tentative support in the pilot study data, which displayed meaningful variations in perceived levels of dread and familiarity in two of the four security risk scenarios.

The use of *affective* words, as the observable and measurable component of an *affect* heuristic, was also tentatively supported by the pilot study data, with meaningful variations in reaction intensity recorded between a number of neutral and negative scenarios. This outcome provided further support for the psychophysiological

argument that words have *affective* qualities that act as stimuli for cognitive processes and objects (Bradley & Lang 1999).

These conclusions drawn from the pilot study data ultimately provided tentative support for the research question – *Does the introduction of affect to the communication of security risk information lead to variations in security risk experts' perceived levels of dread and familiarity?*